UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. TILL KOTTMANN, a/k/a, "deletescape," Defendant.	CASE NO. MJ20-593 **COMPLAINT** Title 18, United States Code, Section 371

BEFORE the Honorable Michelle L. Peterson, United States Magistrate Judge, U.S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT 1

(Conspiracy to Commit Computer Fraud and Abuse)

A. Overview

1. The defendant, TILL KOTTMANN, known by the moniker "deletescape," is a Swiss national who resides in Lucerne, Switzerland.

2. KOTTMANN, a self-proclaimed "hacktivist,"[1] is a member of a group of cybercriminal actors engaged in the hacking of protected computer networks of corporate

[1] The term "hacktivist" generally refers to a person who gains unauthorized access to computer files or networks in order to further a personal, social, or political agenda.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and governmental entities and in the public dissemination of confidential and proprietary information, including source code and internal user data.

3. KOTTMANN conducted intrusion activity, using a variety of techniques, and predominantly has targeted "git" repositories belonging to companies in various countries, including the United States, among others. "Git" refers to a distributed version-control system for tracking changes in source code during software development in containers called repositories. It is designed for coordinating work among programmers, but it can be used to track changes in any set of files. GitLab, Gitea, and GitHub are examples of systems that use "git" repositories. Accordingly, KOTTMANN predominantly targets source code and other confidential and proprietary information, which often includes administrative credentials and other means of further system or network access.

4. KOTTMANN further published, or "leaked," victim data obtained through his and his co-conspirators' hacking conduct, as well as victim data provided to him through other like-minded actors. Since at least 2019, KOTTMANN has operated a website called git.rip ("git.rip website"), which supports and facilitates data leaks by providing public access to databases of "Confidential & Proprietary" files and information of corporate and governmental entities. KOTTMANN similarly promotes and disseminates hacked material through an associated Telegram[2] channel, called "ExConfidential," and through a foreign-based file-sharing service.

5. Through such various means, as of September 2020, KOTTMANN has posted data of more than 80 companies and government agencies, which were available publicly for review and download. The published downloadable databases include numerous prominent U.S. companies as well as foreign entities located in Switzerland, Germany, Taiwan, India, China, Ukraine, and Russia, among other countries. The

[2] Telegram is a messaging service that provides for end-to-end encryption.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

owners of the published data (victims) are identified by name and often by corporate logo.

6. In order to drive traffic to his data leak sites and to solicit and recruit the assistance, participation, and collaboration of others, KOTTMANN has utilized various online platforms, including Twitter, to promote his data leaks and hacking conduct. KOTTMANN also has invited contact from journalists and provided interviews to news media outlets.

B. Offense

7. Beginning at a time unknown, but no later than November 2019, and continuing through September 2020, in King County, within the Western District of Washington, and elsewhere, the defendant, TILL KOTTMANN, and others known and unknown, did knowingly and willfully combine, conspire, confederate and agree together to commit offenses against the United States, to wit:

a. to intentionally access a computer without authorization, and exceed authorized access to a computer, and thereby obtained information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States and the laws of a state, including Washington, and the value of the information obtained exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (ii) and (iii); and,

b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to one or more persons during a one-year period aggregating at least $5,000 in value and damage affecting 10 or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

C. Objectives of the Conspiracy

8. The objectives of the conspiracy included, through use of deceptive and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

fraudulent means, gaining access to protected computers and stealing confidential and proprietary files and information stored thereon. The objectives of the conspiracy further included sharing and disseminating stolen confidential and proprietary files and information, all with the purpose and intent to deprive victims of the exclusive control and ownership of their property.

D. Manner and Means of the Conspiracy

9. The manner and means used to accomplish the conspiracy included the following, which further involved use of the Internet and affecting interstate and foreign commerce and communication:

a. The conspirators, including KOTTMANN, accessed protected computers, including vulnerable "git" repositories through use of stolen credentials and exploits allowing expansive permissions to new users.

b. The conspirators, including KOTTMANN, used the access to "git" repositories to survey the content and to copy and clone databases to servers under the custody or control of the conspiracy. The servers used by the conspiracy to store stolen data are located in one or more foreign countries and hosted by foreign-based service providers.

c. The conspirators, including KOTTMANN, solicited others for copies of stolen and hacked data and for access to confidential and proprietary files and information.

d. The conspirators, including KOTTMANN, publicly posted, or leaked, copies of the stolen databases over a variety of channels, including the git.rip website, the associated Telegram channel "ExConfidential," and through a foreign-based file-sharing service, which the conspirators also managed and maintained.

e. The conspirators, including KOTTMANN, promoted the git.rip website and their associated data leaks efforts, through use of multiple online accounts, including Twitter and other social media platforms, and through information provided to news media outlets about their exploits.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

E. Overt Acts

10. In furtherance of the conspiracy, and to achieve the objects thereof, the defendant, and others known and unknown, did commit and cause to be committed, the following overt acts, among others, in the Western District of Washington and elsewhere:

a. On or about November 18, 2019, KOTTMANN, directly or indirectly, registered the git.rip domain at a U.S.-based domain registrar.

b. On about December 20, 2019, KOTTMANN, directly or indirectly, registered and created an account at a U.S.-based cloud infrastructure provider, which KOTTMANN used to host the git.rip website. The databases accessible through the git.rip website were housed on servers located in one or more foreign countries.

c. On about February 14, 2020, KOTTMANN, directly or indirectly, accessed one or more protected computers and copied files of a manufacturer of security devices headquartered within the Western District of Washington ("Victim-1"). KOTTMANN later posted Victim-1's confidential and proprietary source code on the git.rip website.

d. On about April 15, 2020, KOTTMANN, directly or indirectly, accessed one or more protected computers and copied files of a U.S.-based manufacturer of tactical equipment ("Victim-2"). KOTTMANN later posted Victim-2's confidential and proprietary source code on the git.rip website.

e. On about April 28, 2020, as on numerous other occasions, KOTTMANN, directly or indirectly, accessed the administrative account related to the git.rip website.

f. On about May 4, 2020, KOTTMANN, directly or indirectly, posted confidential and proprietary source code of a large technology company headquartered within the Western District of Washington ("Victim-3"), on the git.rip website. Additional Victim-3 data was published on subsequent dates, including by KOTTMANN on or about July 15, 2020.

g. On about May 17, 2020, KOTTMANN, directly or indirectly, sent a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

message ("tweeted") from his Twitter account, namely, account username @deletescape, "i love helping companies open source their code."

h. On about June 11, 2020, KOTTMANN, directly or indirectly, shared a database purporting to belong to a video game developer headquartered within the Western District of Washington ("Victim-4"), on Telegram.

i. On about July 22, 2020, KOTTMANN, directly or indirectly, tweeted from his @deletescape Twitter account a message requesting that persons with "access to any confidential info, documents, binaries or source code, which you think should be made available to the public" contact him using an encrypted messenger service.

j. On about August 6, 2020, KOTTMANN, directly or indirectly, published technical material, code, and documents related to a U.S.-based microchip and processor manufacturer ("Victim-5"). KOTTMANN later tweeted from his @deletescape Twitter account about the leak of Victim-5's files which he claimed to have obtained through "an anonymous source who breached them this year."

k. On about August 10, 2020, KOTTMANN, directly or indirectly, registered an account at Twitter, namely, account username @antiproprietary, after Twitter suspended his @deletescape account for violations of user terms of service. Pinned to the profile page of the @antiproprietary Twitter account were the following statements "Antiproprietary Action," "hacktivist i guess, you probably saw me in the news once," and "definitely not deletescape."

l. On or about August 15, 2020, KOTTMAN, directly or indirectly, published additional victim data to the git.rip website, including internal files and records related to the Washington State Department of Transportation ("Victim-6").

All in violation of Title 18, United States Code, Sections 371.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

And the complainant states that this Complaint is based on the following information:

I, Joel Martini, being first duly sworn on oath, depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed for approximately 3 years. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other cybercrimes. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training in the acquisition and analysis of digital evidence (both network and host based), responding to computer intrusions and other incidents. I currently hold a Bachelor's of Science in Information Systems from Corban University.

2. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately 5 years. As part of that employment, I became familiar with the design and operations of various electronic devices, networks, and websites, including technology described herein.

3. I make this affidavit in support of a criminal complaint establishing probable cause that the defendant, Till Kottmann, has committed violations of federal law, including the offense of conspiracy to commit computer fraud and abuse, in violation of Title 18, United States Code, Section 371, as alleged above.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, FBI computer scientists and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the limited purpose of this criminal complaint and does not set forth all of my knowledge about this matter.

TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **IP Address**: An Internet Protocol address (or simply "IP address") is a unique numeric address used by devices, such as computers and servers, on the Internet. An IP address is often a series of four numbers, each in the range 0-255, separated by periods (e.g., 104.250.138.210). Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses (also known as an IP Block).

b. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. **Source Code:** Source code is the list of human-readable instructions that a programmer writes when developing a program. When completed, a computer can understand and execute these coded instructions as provided by the developer.

d. **Git:** "Git" is a distributed version-control system for tracking changes in source code during software development in containers called repositories. It is designed for coordinating work among programmers, but it can be used to track changes in any set of files. GitLab, Gitea, and GitHub are examples of systems that use "git" repositories.

SUMMARY OF PROBABLE CAUSE

6. The FBI is conducting an investigation into the hacking of various entities' computer databases and the subsequent theft and dissemination of information from those

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

entities, including source code, confidential information, and internal user data. As discussed below, the targets of the investigation include a Swiss national named Till Kottmann, currently residing in Lucerne, Switzerland. Kottmann uses the alias "deletescape" across various online, email, and social media accounts, including Twitter, Instagram, and Facebook. As discussed below, Kottmann is the user of the Twitter accounts associated with username @deletescape, which is currently suspended, and username @antiproprietary

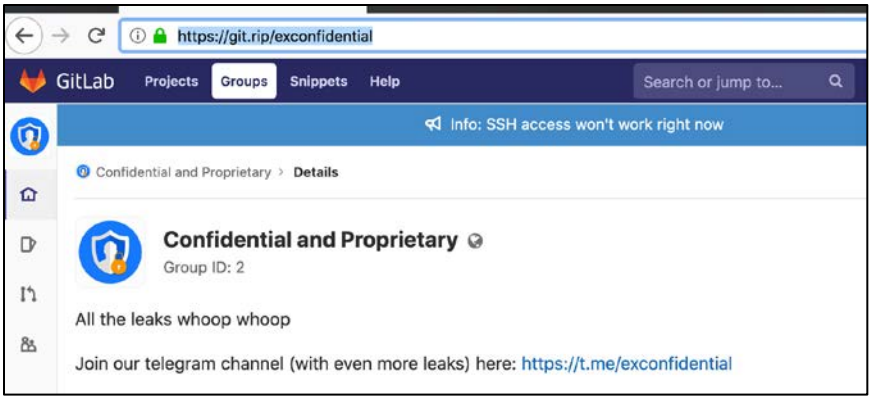
7. Kottmann, who has presented himself as a security researcher, predominantly has targeted "git" repositories and source code belonging to companies in various countries, including the United States, among others. More specifically, Kottmann identified and accessed vulnerable "git" repositories through use of either stolen credentials and/or exploits allowing expansive permissions to new users.[3] Kottmann then copied/cloned their contents to server(s) he controlled and thereafter publicly posted copies of the stolen data to his publicly available, data leaks website http://git.rip ("git.rip website") and/or to his associated Telegram channel "ExConfidential." He also distributed data through Mega, a cloud-based file storage and sharing service provider based in New Zealand. Kottmann also solicited and subsequently posted copies of additional data leaks from others in an effort to promote his website/channel and himself.[4]

8. Kottmann's git.rip website features a webpage (git.rip/exconfidential) that advertises "Confidential and Proprietary" data leaks. A screenshot is below:

[3] By improperly accessing such repositories, Kottmann impaired the integrity or availability of data, a program, a system, or information.

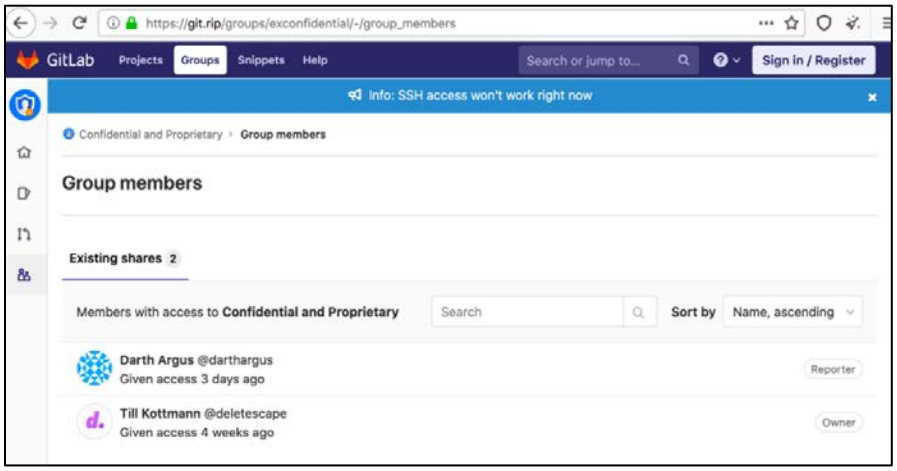
[4] The unauthorized access to protected computers constituted, and was furtherance of, various criminal and tortious acts in violation of state and federal law, including, among others, Revised Code of Washington (RCW) 9A.90.100 (electronic data theft) and 9A.56.150 (possession of stolen property). The conduct under investigation had the effect, and the intended purpose, of depriving the victims of the commercial advantage of the confidentiality and exclusive use of information stored on the protected computers and accordingly providing financial gain to others.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



The git.rip website also invites visitors to join "our" Telegram[5] channel for "even more leaks" and provides a link.

9. The "Users" tab on the git.rip/exconfidential page shows that one member of the site has "Owner" (read/write full admin permissions) access to the global Confidential and Proprietary group. This user has the name Till Kottmann and username @deletescape.



In addition to Kottmann, user @darthargus is listed as having Reporter (read permissions) access to Confidential and Proprietary. Under subgroups, numerous other users have different access privileges, e.g., Maintainer (read/write partial admin permissions).

10. As of September 2020, data dumps from more than 80 entities, including notable companies, are or were available for download on the git.rip website or the

[5] Telegram is a messaging service that provides for end-to-end encryption.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

association Telegram and Mega platform accounts. The published downloadable databases include numerous U.S. companies as well as other foreign entities, including companies located in Switzerland, Germany, Taiwan, India, China, Ukraine, and Russia, among other countries. The git.rip website identifies each victim company database by name and logo.

11. During the course of the investigation, additional entities and apparently hacked data have been added to (and removed from) the git.rip website. For instance,

a. On multiple dates, including on about May 4, 2020, Kottmann posted source code and other data of a large technology company headquartered within the Western District of Washington (Victim-3).

b. On about June 11, 2020, Kottmann posted a database purporting to belong to a video game developer headquartered within the Western District of Washington (Victim-4).

c. On about August 6, 2020, Kottmann published a trove of confidential technical material, code, and documents related to various processors and chipsets of U.S. chip manufacturer (Victim-5). Kottmann later wrote on Twitter about the Victim-5 data: "They were given to me by an anonymous source who breached them earlier this year, more details about this will be published soon."[6]

d. More recently, on about August 15, 2020, additional databases were published on the git.rip website, including internal files and records related to the Washington State Department of Transportation (Victim-6).

12. As part of its investigation, the FBI downloaded and examined samples of the featured data leaks. All of the repositories analyzed appeared to contain source code as advertised. Some of the leaked code further contained passwords, credentials and other items that enabled access to additional company networks or servers. The FBI also interviewed numerous victims, which confirmed the authenticity of their data, including

---

[6] *See, e.g.*, https://www.bleepingcomputer.com/news/security/intel-leak-20gb-of-source-code-internal-docs-from-alleged-breach/ (last visited 08/19/2020).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

proprietary source code, that Kottmann published. Some victims further provided details about the the initial data breach and theft. None of the victims had any association with Kottmann or "deletescape."

13. For example, on April 28, 2020, I met with representatives from Victim-1, a provider of enterprise class safety solutions (such as panic buttons) located in Seattle, Washington. Victim-1 reported that, in April 2020, a former employee discovered what he recognized to be the company's proprietary source code published on the git.rip website. According to Victim-1, the stolen code available on the git.rip website was a mirror of the company's GitLab repository. GitLab is a platform that companies can install on their infrastructure to store their codebase and change it with version control in digital containers called repositories. Victim-1 confirmed that the files on the git.rip website were authentic, relatively recent, private, and electronically stored, indicating that an unauthorized computer intrusion had taken place. After conducting an internal investigation, Victim-1 concluded that a hacker used an exploit in GitLab to gain access to the company's data and clone it to the git.rip website. As evident from activity logs, the hacker created a new user account called "deletescape" to siphon the data on their network.

14. Investigators determined that Victim-1's data was posted to the git.rip website on or about February 14, 2020. Similarly, records obtained from the hosting service provider show that, on the same date, user deletescape (Kottmann) cloned Victim-1's data to the of the git.rip website.[7]

15. Additionally, I have spoken with special agents from FBI Oklahoma City who interviewed representatives of Victim-2, a tactical device manufacturer based in Broken Arrow, Oklahoma. Victim-2 contacted their office to report and confirm that they suffered a data breach similar to that described by Victim-1. One of the repositories

[7] According to Victim-1, the stolen data posted on the git.rip website were hosted through servers in Oregon and Western Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

available on the git.rip website features Victim-2's name and logo.[8] The data was posted on or about April 15, 2020. Similarly, records obtained from the hosting service provider also show that, on the same date, user deletescape (Kottmann) cloned Victim-2's data to the of the git.rip website.

16. Kottmann has openly disclosed and discussed his conduct on various online platforms, including Twitter, and with media outlets. For instance, on about May 17, 2020, Kottmann "tweeted" from his Twitter account @deletescape reference to his hacking and dissemination of companies' private source code:

In other "tweets," Kottmann has solicited others to provide him additional hacked data to leak. For instance on about July 22, 2020, Kottmann expressly invited others with "access to any confidential info, documents, binaries or source code, which you think should be made available to the public," to contact him directly:

He also posted his contact information, which incorporated the moniker "deletescape," and invited media inquiries about his data leaks:

[8] Similarly, other companies confirmed that the published data did indeed come from their servers but were unaware of or unable/unwilling to confirm a prior hack or how the data was stolen.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As reported by media outlets, Kottmann has acknowledged his and his associates' conduct in interviews, although he claimed to take steps to mitigate the damage to the victims from his data leaks.[9] Through these and other messages and through published interviews, Kottmann also confirmed his use of the online alias "deletescape."

17. According to records from a U.S-based domain registrar, the git.rip domain was registered on or about November 18, 2019, by an account in the name of Till Kottmann and username deletescape. In addition to git.rip, the account registered numerous domains, including deletescape.cloud and deletespace.ch.

18. The git.rip website was hosted at a particular IP address, through use of a U.S.-based cloud infrastructure provider. According to records and information related to the associated account, the IP address hosting the git.rip website was created on December 20, 2019, under the name "Deletescape-cloud." Further, the IP address was associated with an account created on August 30, 2019, using IP address 195.245.237.179, and registered to the customer email, me@deletescape.ch, name "Till Kottmann", User ID 6507364, and location of Lucerne, Switzerland. Further, logs of this user's login activity show IP addresses that resolve to SwissCom, a major Internet service provider in Switzerland. The chart below includes descriptions of some of the IP addresses used to access the hosting account and specifically the git.rip database:

---

[9] *See, e.g.*, https://tech.hindustantimes.com/tech/news/swiss-developer-get-access-to-microsoft-nintendo-and-other-big-firm-s-source-codes-revealing-confidential-information-71595925484091.html (last visited 08/09/2020); https://www.bleepingcomputer.com/news/security/source-code-from-dozens-of-companies-leaked-online/ (last visited 08/09/2020).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

IP	Date(s)	Provider	Relevance
195.245.237.179	2019-08-30 13:46:06 UTC	Fenaco Genossenschaft	Account creation Account login activity
178.197.235.208	2020-01-08 20:06:12 UTC	Swisscom AG	Account login activity
83.79.177.129	2020-01-09 20:06:01 UTC	Swisscom AG	Account login activity
85.1.85.224	2020-03-10 09:40:26 UTC	Swisscom AG	Account login activity Admin login for git.rip database
92.104.30.47	2020-04-28 03:37:00 UTC	Bluewin; Swisscom AG	Admin login for git.rip database

Further, four of the five above-listed IP addresses also were used to access the domain registrar account used to register the git.rip domain.

19. According to records from Twitter, Twitter account @deletescape was registered in March 2015, and is associated with email me@deletescape.ch and a Swiss phone number from Swisscom Mobile. Furthermore, according to account login logs, IP address 92.104.30.47, which also was used to conduct activity for the git.rip website (identified above), was used to log into Twitter account @deletescape on numerous (more than 90) occasions between April 1, 2020 and May 1, 2020. These account logins include multiple logins using this same IP address on April 28, 2020, the same date the IP address was used for admin access of the git.rip database.

20. On about August 10, 2020, I discovered that account @deletescape had been suspended by Twitter, apparently for violations of the platform's terms of service. Although the basis for this account action is unknown to me, this suspension appears to have occurred shortly after Kottmann tweeted about his data leak from the well-publicized hack of Victim-5.

21. Through further investigation, investigators identified another, recently-created Twitter account that appeared to be used by Kottmann, specifically, Twitter username @antiproprietary. As set forth in the screenshot below, Twitter account @antiproprietary was created in August 2020, notably approximately when @deletescape was suspended, and referenced Kottmann's known moniker "deletescape" (albeit stating "definitely not deletescape"):

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The account also uses the screenname "Confidential & Proprietary," which is a phrase that likewise appeared on the git.rip website, and acknowledged the user's hacking activity and "Antiproprietary Action." The user (Kottmann) refers to himself as a "hacktivist," which is a term that commonly refers to a person who gains unauthorized access to computer files or networks in order to further an agenda and/or social or political ends.[10]

22. Activity from Twitter account @antiproprietary also indicates that the account user is the same user of @deletescape (Kottmann). For instance, on August 10, 2020, Twitter account @antiproprietary sent a series of tweets referencing "deletescape," including substantively identical messages previously posted by @deletescape. Those included, among others, (i) a tweet identifying his contact information, which incorporated the "deletescape" moniker and invited media inquiries, and (ii) a tweet soliciting source code:

[10] *See, e.g.*, https://en.wikipedia.org/wiki/Hacktivism (last visited 08/19/2020)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

***

He also posted (likely sarcastically) about "not" being @deletescape, and @antiproprietary "not" being used to evade a "ban," which appears to be reference to the account suspension of his Twitter account @deletescape:

23. On August 12, 2020, Twitter account @antiproprietary (Kottmann) posted (possibly jokingly) about arguing that his and his associates' ("me hacking corps") hacking activity and publication of stolen data amounted to a form of free speech:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Based on my training and experience, I am familiar with this ideology, which exists among certain hacktivists.

24. Investigators have requested subscriber records for Twitter account @antiproprietary, but to date responsive data has not yet been received and reviewed. However, there is ample probable cause to conclude that the user of both accounts are the same person and that that person is Kottmann.

25. Based on the investigation, including analysis of the published data and interviews with victims, there is probable cause to conclude that the value of the information taken is extremely high, potentially in the millions of dollars and far in excess of $5,000 within a one-year period, and that the conduct caused damage affecting far in excess of 10 protected computers.

CONCLUSION

Based on the above facts, I respectfully submit that there is probable cause to believe that TILL KOTTMANN did knowingly and intentionally commit the offense of conspiracy to commit computer fraud and abuse, in violation of Title 18, United States Code, Section 371.

JOEL MARTINI, Complainant
Special Agent, FBI

The above agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 15th day of September, 2020. Based on the Complaint and the sworn statement, the Court hereby finds that there is probable cause to believe the Defendant committed the offenses set forth in the Complaint.

MICHELLE L. PETERSON
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970